Discrete Applied Mathematics 39 (1992) 155–159
North-Holland

Note

Generating bent sequences

C.M. Adams* and S.E. Tavares

Department of Electrical Engineering, Queen's University at Kingston, Kingston, Ont., Canada K7L 3N6

Received 8 August 1989
Revised 13 November 1991

Abstract

Adams, C.M. and S.E. Tavares, Generating bent sequences, Discrete Applied Mathematics 39 (1992) 155–159.

We introduce two general classes of bent sequences, "bent-based" and "linear-based", and conjecture that all bent sequences fall into these classes. This gives us a framework for discussing the construction and cardinality of the set of bent sequences of any given order.

Introduction

Let $n=2^m$ for m a positive even integer. For each vector x in $Q_n=\{1,-1\}^n$, let $\hat{x}=(1/\sqrt{n})H_m x$, where

$$H_m=\bigotimes_{i=1}^{m}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

is the Walsh–Hadamard matrix of order n and $\otimes$ is the Kronecker (or tensor) product. We are interested in generating vectors x in Q_n for which $\hat{x}$ is also in Q_n. Such vectors x are known as bent vectors or *bent sequences*.[1]

Correspondence to: Professor Tavares, Department of Electrical Engineering, Queen's University, Kingston, Ont., Canada K7L 3N6.

* Current address: Bell-Northern Research, Ltd., P.O. Box 3511, Station C, Ottawa, Ont., Canada K1Y 4H7.

[1] Note that a bent sequence in $\{0,1\}^n$ is the sequence of outputs of a bent Boolean function when the inputs are applied in lexicographic order. For the purposes of this paper we map the set of Boolean function outputs $\{0,1\}$ to the set $\{+1,-1\}$ so that bent sequences are elements of Q_n.

We let B_n denote the bent sequences in Q_n. For example, when $m=2$,

$$H_2=\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{bmatrix}$$

and $B_4=\{111-1,\ 11-11,\ 1-111,\ -1111,\ -1-1-11,\ -1-11-1,\ -11-1-1,\ 1-1-1-1\}$. The remaining vectors in Q_4 are linear: $L_4=\{1111,\ 11-1-1,\ 1-11-1,\ 1-1-11,\ -111-1,\ -11-11,\ -1-111,\ -1-1-1-1\}$. The set L_n is easy to construct for any n (L_n consists of the rows of H_m and their complements, so that $|L_n|=2^{m+1}=2n$), however, the construction and cardinality of B_n are unknown in general.

Background information on bent functions and sequences regarding length, weight, specific constructions, applications, and generalizations to larger fields can be found in [8, 2, 11, 7, 10, 5, 12, 3, 4, 6, 1, 13, 9].

Generating and counting bent sequences

We define two general classes of bent sequences:

(i) bent-based bent sequences,

(ii) linear-based bent sequences.

A bent sequence x or order $n=2^m$ is *bent-based* if it is a concatenation of 2^{m-2} bent subsequences of order 4; that is, $x^{\mathrm{T}}=(u_1^{\mathrm{T}}u_2^{\mathrm{T}}\cdots u_{2^{m-2}}^{\mathrm{T}})$ where $u_i=(u_{i_1}u_{i_2}u_{i_3}u_{i_4})\in B_4$ for each i. x is *linear-based* if it is a concatenation of 2^{m-2} linear subsequences of order 4; that is, $x^{\mathrm{T}}=(v_1^{\mathrm{T}}v_2^{\mathrm{T}}\cdots v_{2^{m-2}}^{\mathrm{T}})$ where $v_i=(v_{i_1}v_{i_2}v_{i_3}v_{i_4})\in L_4$ for each i.

Conjecture. Every bent sequence is either bent-based or linear-based.

This conjecture holds for bent sequences in B_4 and B_{16}. We now present simple algorithms which show that such sequences exist and are easy to generate.

Bent-based bent sequences

Theorem. *Let x_1, x_2, x_3, x_4 be in B_n and let z be the concatenation of the transforms of these sequences; that is, $z^{\mathrm{T}}=(\hat{x}_1^{\mathrm{T}}\hat{x}_2^{\mathrm{T}}\hat{x}_3^{\mathrm{T}}\hat{x}_4^{\mathrm{T}})$ in Q_{4n}. The sequence z is in B_{4n} if and only if $\frac{1}{2}(x_1+x_2+x_3+x_4)$ is in Q_n.*

Proof. We write z as an $n\times 4$ matrix: $Z=(\hat{x}_1\hat{x}_2\hat{x}_3\hat{x}_4)$. It is easy to check that

$\hat{z}=(1/\sqrt{4n})H_{m+2}z \Rightarrow \hat{Z}=\frac{1}{2}\cdot(1/\sqrt{n})H_mZH_2$. Therefore,

$$\begin{aligned}\hat{Z} &= \tfrac{1}{2}\cdot\frac{1}{\sqrt{n}}H_m(\hat{x}_1\hat{x}_2\hat{x}_3\hat{x}_4)H_2\\ &= \tfrac{1}{2}(x_1x_2x_3x_4)H_2\\ &= \tfrac{1}{2}XH_2\end{aligned}$$

where $X=(x_1x_2x_3x_4)$. Now, $Z\in B_{4n}$ iff $\hat{Z}=\frac{1}{2}XH_2\in Q_{4n}$. But $X\in Q_{4n}$ since the columns $x_i\in B_n$. The ith row of $\hat{Z}$, $\hat{Z}_i$, $\in Q_4$ iff the ith row of X $\in B_4$; that is, iff $(x_{1_i}+x_{2_i}+x_{3_i}+x_{4_i})=\pm 2$, for all i. Therefore, $\hat{Z}\in Q_{4n}$ iff $\frac{1}{2}(x_1+x_2+x_3+x_4)\in Q_n$. □

The method for creating bent-based bent sequences (BBBS's) should now be clear. To generate a BBBS $z\in B_{4n}$, choose four BBBS's $x_1, x_2, x_3, x_4\in B_n$, such that $\frac{1}{2}(x_1+x_2+x_3+x_4)\in Q_n$ and form $z^{\mathrm{T}}=(\hat{x}_1^{\mathrm{T}}\hat{x}_2^{\mathrm{T}}\hat{x}_3^{\mathrm{T}}\hat{x}_4^{\mathrm{T}})$.

The number of BBBS's in B_{4n} can now be trivially lower-bounded in terms of the number of BBBS's in B_n since $\frac{1}{2}(x_1+x_1+x_1-x_1)\in Q_n$, for all x_1, and $\frac{1}{2}(x_1+x_1+x_2-x_2)\in Q_n$, for all x_1, x_2 where $x_2\neq\pm x_1$. Note that there are four possible orderings of $(\hat{x}_1^{\mathrm{T}}\hat{x}_1^{\mathrm{T}}\hat{x}_1^{\mathrm{T}}-\hat{x}_1^{\mathrm{T}})$ and six possible orderings of $(\hat{x}_1^{\mathrm{T}}\hat{x}_1^{\mathrm{T}}\hat{x}_2^{T}-\hat{x}_2^{\mathrm{T}})$. Therefore, if there are β_n BBBS's in B_n, then there are at least $4\times\binom{\beta_n}{1}+6\times\binom{\beta_n}{1}\binom{\beta_n-2}{1}=4\beta_n+6\beta_n(\beta_n-2)$ BBBS's in B_{4n}. If $x_i\neq\pm x_j$ for $i, j\in\{1,2,3,4\}$ $i\neq j$, then it becomes less clear as to how many ways there are to select four bent sequences for which $\frac{1}{2}(x_1+x_2+x_3+x_4)\in Q_n$ holds. Certainly if there are w ways, then w is some function of β_n and this leads to $w(4!)$ unique bent sequences. We therefore have

$$\begin{aligned}\beta_{4n} &= 4\beta_n+6\beta_n(\beta_n-2)+24w\\ &= 6\beta_n^2-8\beta_n+24w.\end{aligned}\tag{1}$$

Linear-based bent sequences

Yarlagadda and Hershey have pointed out [13] that if H_m is a Hadamard matrix of order n so that $H_m=(h_1h_2\cdots h_{2^m})$, where the h_i are the columns of H_m, then the vector $x^{\mathrm{T}}=(h_1^{\mathrm{T}}h_2^{\mathrm{T}}\cdots h_{2^m}^{\mathrm{T}})$ (i.e., the vector formed by concatenating the columns) is a bent sequence of order n^2. This is because $\hat{x}=x\in Q_{n^2}$. We note that any sequence constructed in this way is a linear-based bent sequence (LBBS), since the columns of the Hadamard matrix H_2 are in L_4 and the columns of H_m for $m>2$ are composed of columns from H_{m-1}. We note further that $Y=H_mDP$ is bent (see also [5]) and hence is also an LBBS, where D is a diagonal matrix with ± 1 on the diagonal and P is a permutation matrix. This is because $\hat{Y}=DPH_m$. Thus $\hat{Y}$ is a Hadamard matrix with rows permuted by P and complemented by the -1 entries in D, implying that $\hat{Y}\in Q_{n^2}$ and therefore that $Y=H_mDP$ is bent. However, Y is

simply a Hadamard matrix with the *columns* permuted and complemented, so the columns of Y remain linear and concatenating these columns yields a bent sequence which is linear-based.

Counting the LBBS's of a given order is a trivial matter: for matrices of size $n \times n$, there are 2^n possible D matrices (two choices for each diagonal element) and $n!$ possible P matrices. All of these will lead to unique LBBS's, so we have #LBBS's in $B_{n^2} = 2^n \times n!$.

Conclusions

We have defined two classes of bent sequences, bent-based bent sequences (BBBS's) and linear-based bent sequences (LBBS's), and have extended previous work by Yarlagadda and Hershey to give explicit algorithms for constructing sequences in these classes. We have conjectured that every bent sequence belongs to one of these two classes. Our construction of elements of the set B_n leads to a conjecture for a lower bound on the cardinality of this set. We note that for bent sequences in B_{16}, the algorithms yield 512 BBBS's and 384 LBBS's, or 896 bent sequences in total; exhaustive search of all elements of Q_{16} has shown that this is a complete list. For sequences in B_{64} we calculate 37,879,808 BBBS's and 10,321,920 LBBS's, or 48,201,728 bent sequences in total. Although an exhaustive search through all elements of Q_{64} is computationally infeasible, it would be interesting to find out whether this is again a complete enumeration.

We list as an open research problem the search for a good method for calculating w in equation (1). Using the weight of a bent sequence and the requirement that $\frac{1}{2}(x_1 + x_2 + x_3 + x_4) \in Q_n$, we see that w is upper-bounded by $2 \times \binom{\beta_n/2}{3}$; in fact, for $x_i \in B_4$ ($\beta_4 = 8$) this bound is exact. We conjecture that w may be lower-bounded by $2 \times \binom{\beta_n/2}{2} = (\beta_n/2)(\beta_n/2 - 1)$ for $\beta_n > 8$ but this is unproven.

Acknowledgement

The work described in this paper was partially supported by a grant from the Natural Sciences and Engineering Research Council of Canada. We would also like to thank Dr. David Gregory for his helpful comments.

References

[1] H. Chung and P.V. Kumar, A new general construction for generalized bent functions, IEEE Trans. Inform. Theory 35 (1989) 206-209.

[2] J.F. Dillon, Elementary Hadamard different sets, PhD thesis, University of Maryland, College Park, MD (1974).

[3] P.V. Kumar and R.A. Scholtz, Bounds on the linear span of bent sequences, IEEE Trans. Inform. Theory 29 (1983) 854–862.

[4] P.V. Kumar, R.A. Scholtz and L.R. Welch, Generalized bent functions and their properties, J. Combin. Theory Ser. A 40 (1985) 90–107.

[5] A. Lempel and M. Cohn, Maximal families of bent sequences, IEEE Trans. Inform. Theory 28 (1982) 865–868.

[6] V.V. Losev, Decoding of sequences of bent functions by means of a fast Hadamard transform, Radiotekhn. i Elektron. 7 (1987) 1479–1492.

[7] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes (North-Holland, Amsterdam, 1977).

[8] R. McFarland, A family of difference sets in noncyclic groups, J. Combin. Theory Ser. A 15 (1973) 1–10.

[9] W. Meier and O. Staffelbach, Nonlinearity criteria for cryptographic functions, in: Proceeding of EUROCRYPT '89, Advances in Cryptology (Springer, Berlin, 1990) 549–562.

[10] J.D. Olsen, R.A. Scholtz and L.R. Welch, Bent-function sequences, IEEE Trans. Inform. Theory 28 (1982) 858–864.

[11] O.S. Rothaus, On "bent" functions, J. Combin. Theory Ser. A 20 (1976) 300–305.

[12] R. Yarlagadda and J. Hershey, A note on the eigenvectors of Hadamard matrices of order $2**n$, Linear Algebra Appl. 45 (1982) 43–53.

[13] R. Yarlagadda and J.E. Hershey, Analysis and synthesis of bent sequences, IEE Proc. E 136 (1989) 112–123.